IstroSec

Data Sheet

Simulácie útokov

Spoločnosť IstroSec ponúka možnosť otestovať účinnosť a efektivitu bezpečnostných opatrení prostredníctvom simulovaných útokov. Takýmto spôsobom je možné overiť, či zamestnanci majú dostatočné povedomie o kybernetických hrozbách, či sú schopní odolať týmto hrozbám a či Vaše preventívne, detekčné a reaktívne opatrenia fungujú. Ponúkame simulácie útokov sociálnym inžinierstvom a simulácie útočníka v infraštruktúre.

„Počas takejto simulácie útoku sa preverí, či je tím zodpovedný za riešenie incidentov schopný dostatočne rýchlo a účinne reagovať na incidenty."

Simulácie sociálneho inžinierstva:

- Phishing
- Vishing
- Spearphishing
- Smishing
- Whaling
- Fyzické sociálne inžinierstvo

Simulácie útokov sociálnym inžinierstvom

Komplexnú odolnosť voči útokom sociálnym inžinierstvom je možné docieliť vyspelým vzdelávacím programom zamestnancov, adekvátnymi technickými opatreniami a pravidelným testovaním ich efektívnosti. Spoločnosť **Istro**Sec je pripravená pomôcť Vám zvýšiť pripravenosť a odolnosť voči týmto typom útokov.

Simulácie phishingu

Naši experti pripravia a vykonajú phishingovú kampaň, ktorá nebude špecificky cielená na konkrétnych zamestnancov alebo používané technológie či služby. V rámci tejto kampane bude vyhotovený zoznam emailových adries zamestnancov na základe verejne dostupných dát. Následne bude na tieto adresy odoslaný phishingový email snažiaci sa vylákať prihlasovacie údaje, osobné údaje alebo iné citlivé informácie či stiahnuť prílohu.

Simulácie spearphishigu

Pokročilejším a efektívnejším útokom je spearphishing. V rámci tejto simulácie naši experti využívajú open source intelligence (OSINT) na získanie dát potrebných na prípravu cielenej a vysoko účinnej kampane, ktorá bude zohľadňovať špecifiká Vašich technológií, zamestnancov či využívaných služieb. Využívajú sa veľmi podobné domény, obchádzanie multifaktorovej autentifikácie či špecifický malvér napísaný našimi analytikmi malvéru.

Whaling

V rámci simulácií útoku typu whaling naši experti vykonajú spearphishingovú kampaň zameranú na najvyššie vedenie organizácie. Práve útok na túto skupinu osôb môže organizácii spôsobiť značné škody kombináciou ich prístupu ku kritickým informáciám a dynamickým štýlom práce.

Vishing

Telefonické phishingové útoky môžu byť v prípade schopného útočníka veľmi účinným spôsobom ako vylákať citlivé informácie od zamestnancov. Naši experti uskutočnia takýto telefonický útok za použitia informácií z OSINT a využitia psychologickej manipulácie, impersonácie a podvodných trikov.

Smishing

Vašim zamestnancom rozpošleme phishingové SMSky s cieľom vylákať prihlasovacie údaje, osobné údaje alebo iné citlivé informácie či stiahnuť prílohu.

Fyzické sociálne inžinierstvo

Naši experti navštívia Vaše pracovisko a prostredníctvom komunikácie so zamestnancami sa budú snažiť získať informácie využiteľné na podnikanie ďalších útokov, nainštalovať škodlivý softvér, získať heslá, citlivé údaje, alebo prinútiť zamestnancov vykonať aktivitu, ktorá porušuje bezpečnostné politiky organizácie.

Simulácia útočníka v infraštruktúre

Simulácie špecifických aktivít útočníka

Simulácie špecifických aktivít útočníka v organizácií môžu pozostávať z činností ako napríklad lateral movement, šírenie škodlivého kódu, zber a exfiltrácia dát, obchádzanie bezpečnostných opatrení v organizácií a podobne.

Simulácia komplexného útoku na organizáciu

V rámci tohto typu simulácie otestujeme detekčné a reakčné schopnosti Vášho bezpečnostného tímu na taktiky, techniky a postupy (TTP) pokročilých útočníkov (APT). V prípade, ak sa konkrétna APT skupina aktuálne zameriava na Váš sektor podnikania, vieme Vám pomôcť so zvýšením schopnosti odolať jej špecifickým TTP. Napríklad v prípade skupiny APT41 by mohlo ísť o spearphishing so škodlivou prílohou, WMI, plánované úlohy, PowerShell, DLL Side-Loading, SMB/Windows Admin Shares, keylogging, či zašifrovanie dát ako úniková stratégia.

Prečo IstroSec?

Okrem vysokej kvalifikovanosti pri vykonávaní samotných simulácií, experti IstroSec dôkladne študujú taktiky, techniky a postupy používané útočníkmi v praxi. Vďaka tejto kombinácii môže klient bezpečným spôsobom otestovať svoju odolnosť a pripravenosť na reálne útoky.

Prípadová štúdia

Typ organizácie: finančná inštitúcia
Poskytnutá služba: simulácia spearphishingu
Riešenie: Spearphishing test a vytvorenie malvéru

Organizácia mala záujem o overenie konfigurácie už nasadených ochrán mailového riešenia, taktiež správania sa všetkých zamestnancov v prípade že sa im do firemnej emailovej schránky dostane nevyžiadaná pošta. Z pohľadu služieb bolo možné takýto prípad otestovať využitím služieb spoločnosti **Istro**Sec ako je napríklad simulácia phishingu, alebo ako v tomto prípade, cielenou a účinnejšou spearphishingovou kampaňou.

Zahŕňalo to získanie informácií v úvodnej fáze (reconnaissance) o firme a zamestnancoch, vďaka čomu sme vedeli získať emailové adresy zamestnancov, informácie o mailovej infraštruktúre, používaných ochranách a ďalšie. Následne prebehla príprava kampane ktorá môže obsahovať link na web ktorý bude simulovať originálny web na získanie prístupových údajov a druhého faktoru, prípadne tvorbu malvéru pre potreby sofistikovanej kampane ktorá dokáže odsimulovať ransomware, alebo inú formu správania sa reálneho útočníka.

Počas vytvárania payloadu dochádza k návrhu výsledného emailu ktorý bude následne rozposlaný vybranej skupine zamestnancov, vo vopred definovaný čas. Po rozposlaní kampane dochádza k analýze výsledkov, pričom po ukončení, dochádza k odovzdaniu finálnej správy zákazníkovi. Report obsahuje manažérske zhrnutie, identifikované slabé miesta, detailné štatistiky ako počet odoslaných emailov, kliknutí na link, odoslaných údajov, z akých zariadení sa pristupovalo na phishingový web a ďalšie.